UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X
UNITED STATES OF AMERICA,

MEMORANDUM
AND ORDER

06 CR 31 (SLT)

-against-

AHMED ALDEEN,

Defendant.
----------X
TOWNES, U.S.D.J.

Defendant Ahmed Aldeen ("Defendant" or "Aldeen") moves this Court for an order requiring the government to provide him with a mirror image of the computer hard drive – allegedly containing images of child pornography – that formed the basis for his arrest for violating 18 U.S.C. § 2252(a)(5)(B). Based on the submission of the parties, and oral argument held on March 3, 2006, and for the reasons stated below, Defendant's motion is granted, subject to a protective order prohibiting viewing of the subject videos by anyone other than defense counsel and mandating that any pornographic files be destroyed or returned to the government at the conclusion of this case.

I. *Statement of Facts*

During the course of an unrelated investigation on November 26, 2005, the United States Secret Service discovered two seven-minute video files containing video images of a young girl being sodomized and molested by an adult male on the hard drive of a computer possessed by Aldeen. Operating system data revealed that the videos were downloaded on October 2, 2005,

and October 12, 2005, and were most recently accessed on November 11, 2005, and November 18, 2005, respectively. Though the computer containing the images belonged to Aaron Harp, Defendant Aldeen admitted that he maintained possession over the computer from April 2005 until approximately November 18, 2005, when he returned it to Harp. On the basis of these facts, Defendant Aldeen was indicted for two counts of possessing child pornography in violation of 18 U.S.C. § 2252(a)(5)(B). (*See* Indictment.)

Defendant now requests, pursuant to Federal Rule of Criminal Procedure 16 (a)(1)(E) ("Rule 16"), that he be provided with a copy of said images because, he argues, they are material to the preparation of his defense. Additionally, Defendant argues:

> we must determine who had access to the computers seized by the government, when the images were stored in those computers, whether and when the hard drives were altered, what access the computer operators had to the Internet and with whom they conversed, whether the hard drives contained viruses, the ages of the alleged minors depicted in the videos, the exact behavior of those minors, and whether the videos traveled in interstate commerce.

(Colson Letter Mot. at 2.)

In response to Defendant's initial request for the videos, the government presents the Defendant with several options. It agrees to provide Defense Counsel and the relevant experts (the "Defense Team") with a mirror image of the hard drive, save the two video files in question. (Bitkower Letter Mot. at 2.) Alternatively, the Defense Team may view the videos during regular business hours at the Secret Service office in Brooklyn either in the presence of a Secret Service official, or in a private room, subject to a search of the Defense Team by a Secret Service official upon departure. (*Id.*) The government argues that the Defendant is entitled to no greater access to the materials, as they are contraband, the reproduction of which is illegal.

Defendant responds that (a) the type of analysis planned by the Defense Team's computer experts is complex and would be burdensome to perform at the Secret Service office; (b) the government will have unfair access to their work product; (c) the Defense Team cannot bear the cost of transportation to and from the Secret Service office for those who will need access; and (d) that attorneys from the Federal Defender's office covering the Southern District of New York have received similar materials in the past without any foul play or illegal duplication or distribution. (Colson Letter at 3-4.)

II. *Discussion*

Rule 16 provides, in relevant part:

> Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or potions of any of these items, if the item is within the government's possession, custody and control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant.

Fed. R. Crim. P. 16(a)(1)(E).

Child pornography is illegal contraband. 18 U.S.C. § 2252A(a)(5)(B); *New York v. Ferber*, 458 U.S. 747 (1982). Though the Second Circuit has yet to address the question of whether, in order to prepare for trial, a defendant is entitled to copies of pornographic images obtained from him, two other circuits have ruled in favor of the government on this same issue.

In *United States v. Kimbrough*, 69 F.3d 723 (5th Cir. 1995), the government refused to copy the pornography in question but offered to take the videos to the defendant's expert and allowed the defense team access to the videos at the United States Customs Service office, the

United States Attorney's office or defense counsel's office. *Id.* at 731. The Fifth Circuit rejected defendant's argument that the government's refusal to permit copying of the tapes constituted a violation of his constitutional rights to due process and effective assistance of counsel: "The Government's offer to make the materials available for inspection but not allow them to be copied was reasonable. Furthermore, Kimbrough has failed to demonstrate that any actual prejudice arose from his inability to procure copies of the charged items." *Id.*

In *United States v. Horn*, 187 F.3d 781 (8th Cir. 1999), the Eighth Circuit rejected defendant's argument on appeal that he was entitled to have copies of pornographic tapes for the benefit of his expert witness. *Id.* at 792. The court found that the government's willingness to have the would-be expert view the original copies would satisfy Rule 16 without duplicating contraband. *Id.* The court specifically highlighted defendant's failure to show how he was prejudiced by the trial court's refusal to order that the videos be copied. *Id.* However, the court declined to address defendant's argument that he could have used a copy of the tape in his defense (to contact the producers thereof and identify the age of the performers), since defendant failed to raise it with the trial court. *Id.* 792-3 ("In a proper case, and perhaps after a sufficient preliminary showing, such a rationale might well have required the trial court to grant [defendant's] discovery motion. But [defendant]...never advanced this rationale to the trial court."); *see also United States v. Husband*, 246 F. Supp. 2d 467, 468-8 (E.D. Va. 2003) (denying defendant's motion for a copy of pornographic materials, citing *Kimbrough* and *Horn*, and holding that private room for viewing by defense team is sufficient); *United States v. Cox*, 190 F. Supp. 2d 330, 334 (N.D.N.Y. 2002) ("Defendant provides no factual basis for his assertion that physical possession of the government's evidence is necessary to adequately

prepare his defense nor does he cite legal authority which suggests he is entitled to return of the illegal materials.").

Some district courts have addressed this question and ruled in favor of the defendants. In *United States v. Frabizio*, 341 F. Supp. 2d 47 (D. Mass. 2004), defendant argued that his defense team was entitled to a copy of the pornographic video forming the basis of his arrest. Defendant claimed that "making trips to the FBI location [would] be burdensome," that "the government's proposal prevents defense counsel from consulting freely with her expert" and that "any tests conducted on an FBI computer will leave behind a roadmap of the process and its results on that computer's hard drive," giving the government access to defendant's work product. *Id.* at 49. The court granted defendant's motion and adopted a protective order limiting the inspection of the images to defense counsel and prohibiting examination of those images on any computer connected to a network. *Id.* at 49. The Court found no reason to believe that defense counsel could not be trusted to adhere to these requirements. *Id.* at 51.

Fabrizio relied heavily on *United States v. Hill*, 322 F. Supp. 2d 1081 (C.D. Ca. 2004), in which the court ordered the government to provide defense counsel with a copy of the images forming the basis of the government's case against the defendant. In *Hill*, the court found that the government's offer (permitting the defense expert to analyze the media in the government's lab at scheduled times, in the presence of a government agent) inadequate: "[t]he defense experts needs to use his own tools in his own lab. And he cannot be expected to complete his entire forensic analysis in one visit to the FBI lab." *Id.* at 1092. Furthermore, the found that "not only does defendant's expert need to view the images, his lawyer also needs repeated access to the evidence in preparing for trial." *Id.*

In *United States v. Kirzhner*, No. 02-CR-387, slip op. (E.D.N.Y. Jun. 14, 2002) (Garaufis, J.), defendant requested a copy of the pornographic images he allegedly possessed "for the limited purpose of permitted a medical expert to review the depictions in order to assist in preparing Defendant's case." (Order of June 12, 2002 ("June 12 Order") at 2.) Judge Garaufis found that "[w]hen a defendant is charged with a crime based on his or her transportation of images that allegedly constitute child pornography, the images themselves are clearly 'material to the preparation of the defendant's defense.'" (June 12 Order at 5.) *Kirzhner* distinguished both *Kimbrough* and *Horn* based on the failure of the defendants in both cases to demonstrate undue prejudice if not given a copy of the videos, and pointed out that under *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 258 (2002), which found overbroad a statute banning virtual child pornography, "many defendants charged with child pornography crimes will seek expert analysis of the images that form the basis of the charges against them in order to determine whether the images constitute actual child pornography or whether they are constitutionally protected virtual images." June 12 Order at 5 n.2; *see also Ashcroft v. Free Speech Coalition*, 535 U.S. at 258. Judge Garaufis ordered the government to provide defense counsel with a copy of the images, subject to many restrictions. (June 12 Order at 6-7.)

This Court recognizes the need to prevent duplication of child pornography. *See Ashcroft*, 535 U.S. at 249 ("Like a defamatory statement, each new publication of the speech would cause new injury to the child's reputation and emotional well-being."). However, the two Circuit Court cases upon which the government has asked this Court to rely are distinguishable on significant grounds. In *Kimbrough*, the prosecution offered to supply the images to defense counsel at his office. *Kimbrough*, 69 F.3d at 731. In *Horn*, the defendant waited until his appeal

to argue that he would suffer any prejudice without independent access to the pornography at issue. *See Horn*, 187 F.3d at 792-3. On the contrary, when a defendant can present a compelling reason why his defense team should not be restricted to viewing the alleged pornography on government property, courts have permitted the material to be duplicated, subject to a protective order limiting those who may view the materials and under what conditions.

In the case at hand, the Court finds persuasive Defendant's claims that his computer experts require use of their own computers and two computer programs (Encase and FTK) in order to examine the videos; that examination by computer experts may take many visits to the Secret Service office; and that members of the Federal Defenders' office have tried cases in the Southern District of New York and been provided with similar material under protective orders without incident. (Colson Letter at 2, 4.) At oral argument, Defendant produced his computer expert, Fred Havemann ("Havemann"), who testified that the process of indexing the hard drive of the computer could take up to 48 hours. (Transcript of 3/3/06 Oral Argument ("Tr.") at 4.) While Havemann might be able to tend to other assignments while simultaneously indexing a hard drive at the Federal Defender's office, he (or someone else) would be required to check on the computer periodically at the Secret Service office, and, in the event of a crash (which Havemann claims is a likely occurrence), return to re-start the program. (Tr. at 15-16.) Furthermore, the Court finds noteworthy Havemann's testimony that he and his assistant are the only computer experts covering five Public Defenders' offices, and finds compelling his testimony that a laptop computer would be unsuitable for executing the Encase and FTK programs because laptops are prone to overheating and would likely overheat if left running for 24-48 hours. (Tr. at 16.) In total, denying Defense Counsel a copy of the hard drive would

require the Defense Team to bring a desktop computer to the Secret Service office, have a member of the Federal Defenders' office visit periodically to make sure the program has not crashed and have Havemann or his assistant return to restart the program if it does, and have anyone who wishes to access the hard drive travel from Defense Counsel's downtown Manhattan office to downtown Brooklyn.

Under these circumstances, the Court finds that Defendant has demonstrated an adequate amount of inconvenience if his Team is not provided with a copy of the entire hard drive.

However, to address the government's concern that if Defense Counsel receives a copy of the images, there will be a risk of further duplication and dissemination – a concern that this Court shares – the following restrictions apply:

(1) Only Defense Counsel may examine the materials;

(2) All materials containing government-containing contraband shall be kept by Defense Counsel in a secure, locked room accessible only to Defense Counsel, legal assistants, investigators, and defense experts;

(3) No other person shall examine this material without further court order. No additional copies of this material shall be made without further court order;

(4) Any computer used to analyze the materials shall be a "stand alone" computer, not connected to any network;

(5) The defense shall return to the government or destroy any material deemed contraband by this Court at the conclusion of this case.

III. *Conclusion*

The government shall provide the defense with copies of all materials seized in this case including, but not limited to, mirror images of any and all computer hard drives, computer discs, CD Roms, videos, pictures, e-mail messages, instant messages, chat room dialogues, and advertisements. The government shall also make clear which of these items contains material the government believes is contraband. To prevent unauthorized duplication and distribution of the images, release of the images is subject to the accompanying protective order.

SO ORDERED.

Dated: March 16, 2006
Brooklyn, NY

SANDRA L. TOWNES
UNITED STATES DISTRICT JUDGE